STAFF SUMMARY SHEET

	TO	ACTION	SIGNATURE (Surname), GRADE AND DATE		TO	ACTION	SIGNATURE (Surname), GRADE AND DATE
1	DFx	sig	26Feb14 Timothy Pettit, Lt Col FOR	6			
2	DFER	approve	Sozzi, AD-22, 27 Feb 14	7			
3	DFx	action	Jason Belvill, Capt, Originator	8			
4				9			
5				10			

SURNAME OF ACTION OFFICER AND GRADE	SYMBOL	PHONE	TYPIST'S INITIALS	SUSPENSE DATE
JASON BELVILL, 0-3	USAFA/DFM	719-333-2315	JEB	20140228

SUBJECT: Clearance for Material for Public Release — USAFA-DF-PA- 131

DATE: 20140226

SUMMARY

1. PURPOSE. To provide security and policy review on the document at Tab 1 prior to release to the public.

2. BACKGROUND.
Authors: Benjamin Vowell, William Vine, Derek Sandblom

Title: Secure Enclaves Written Submission for NSIC

Circle one: Abstract Tech Report Journal Article Speech Paper Presentation Poster Thesis/Dissertation Book Other: 5 page written submission to NSIC

Check all that apply (For Communications Purposes):
[] CRADA (Cooperative Research and Development Agreement) exists
[] Photo/ Video Opportunities [] STEM-outreach Related [] New Invention/ Discovery/ Patent

Description:
Written submission for NSIC, 25 April

Release Information:
This is a mandatory submission requirement to apply and compete at the National Security Innovations Competition.

Recommended Distribution Statement: Distribution A: approved for public release, distribution unlimited

3. DISCUSSION.
Written submission attached.

4. RECOMMENDATION. Sign Coord block above indicating document is suitable for public release. Suitability is based solely on the document being unclassified, not jeopardizing DoD interest, and accurately protraying official policy.

JASON BELVILL
Instructor of Management

Attachment:
1. Written Submission

Secure Enclaves-Enabled Technologies

TEAM MEMBERS: Derek Sandblom, William Vine, Benjamin Vowell
Team Advisor: Capt Nick Mastronardi
UNITED STATES AIR FORCE ACADEMY

Introduction

Secure Enclaves-Enabled Technologies is a digital security firm to be launched in the coming year. It is born from a unique relationship between Intel Labs and the Department of Homeland Security seeking to develop a revolutionary solution to cyber security problems. In today's increasingly-digital world, hackers and security companies have engaged in a consistent battle of software development to secure data. However, data at rest remains extremely vulnerable. SE Technologies' software goes a layer deeper, activating a hardware solution to put a stop to the death spiral. Utilizing the silicon of the computer chip to create a virtual "fingerprint", our hardware solution will put customers at ease about their organizations' electronic data security. In fact, an NSA "red team" of hackers could not even begin to crack this technology when given the chance.

With the continual evolution of offensive attack techniques, the need for more impressive defensive counter-measures is becoming apparent. As the requisite to fill this capability gap grows, so does the opportunity for businesses. Replacing the need for a counter-measure, recent developments in micro-processer technology have allowed for a veritable impenetrable fortress to be placed inside modern day computer systems.

Few digital security solutions on today's market are hardware based, and none offer this level of security. According to a March 2013 Worldwide Threat Assessment, the number one global threat to the United States is cyber-attack. Recent attacks have revealed protected information, shut down banks and stock exchanges, and have the potential to disrupt and disable critical infrastructure such as power generation [1].

The United States desperately needs a solution to this existing and rapidly-developing security threat and that solution is Secure Enclaves-Enabled Technologies.

Technical Analysis

SE Enabled Technologies provides a critical software complement to revolutionary cyber security hardware developed by Intel. Intel has created a hardware solution for securing data that has no known exploits. A hardware solution to cyber security is unique in an industry dominated by software solutions which hackers inevitably find ways to circumnavigate. Intel states, "Even diligent use of correct software design and implementation practices, can allow secrets to be exposed through a single flaw in any of the privileged code on the platform, code which may have been written by thousands of developers from hundreds of organizations throughout the world" [2].

To address this area of growing concern Intel developed Software Guard Extensions (SGX). The premise behind SGX is the creation of "enclaves" using a new set of CPU instructions. "An enclave is a protected area in the application's address space which provides confidentiality and integrity even in the presence of privileged malware. Attempted accesses to the enclave memory area from software not resident in the enclave are prevented even from privileged software such as virtual machine monitors, BIOS, or operating systems" [3]. Typically, malicious software gains access through exploiting flaws in code which give it access to privileged software. Once the malicious code has gained access to that privileged software, it has the necessary access to exploit all other applications on the operating system. The capabilities provided by SGX mean that even if the OS or other highly privileged software is exploited by malicious software, the code and data contained in the enclave will remain secure.

Applications can be loaded into and run inside of the enclaves. Once the loading of the application's code and data is complete, the enclave is sealed and all other external forms of software access are denied [4]. This ultimately allows for the "control of the security of sensitive code and data by creating trusted domains within applications to protect critical information during execution and at rest" [5].

SGX uses access control mechanisms built into the processor to prevent unauthorized software access. Even when data leaves the enclave to be written to memory, the data is kept secure through automatic encryption and integrity protection [6]. Additionally,

multiple enclaves can be created within systems allowing for the separation of "secrets" from one another. For example, medical data could be secured separately from banking data.

SGX will be a standard component of Intel's chipsets beginning in 2015. However, new software must be developed or current software must be adapted in order to have the ability to utilize the new set of instructions provided by the chipset. Without this critical software development, the cyber security solution afforded by SGX will lie dormant.

SE Enabled Technologies seeks to exploit the capabilities of SGX through the creation of software solutions. Currently, we are seeking to compliment Intel's hardware solution through the use of a browser extension application. Using the browser extension, we can offer a wide array of security solutions from secure storage and transmission of documents to secure video streaming. The potential applications of this software are numerous and lucrative. For example, an organization such as the Department of Veteran Affairs could us SE Enabled software to securely transmit PII of patients, keep financial data safe, and conduct protected communications between various extensions of the department. The combination of SE Enabled Technologies software and Intel's SGX has the potential to revolutionize the cyber security landscape and to bring relief to a problem plaguing major government and public sector organizations throughout the world today.

Implementation Readiness Analysis

Cyber security and the extreme risks associated with exploitation no longer dwell in the realm of science fiction. SE Enabled Technologies will focus its efforts in two different market segments: large business organizations and, eventually, individuals. The current federal market for digital security solutions is over $63 billion dollars, and is steadily growing [7]. It is forecast to continue rapidly expanding into the next decade. The space is broken down between agencies and could further be expanded to the private sector beyond government contractors.

The main focus of Secure Enclaves-Enabled Technologies is large business organizations within the national security realm. A large business is being described as a business or government organization with a minimum of 250 devices.

The market need for security software that protects sensitive information is obvious. Corporations are making the news when their servers fall prey to hackers, who steal millions of customers' personally identifiable information. In the recent breach of Target's infrastructure, over 70 million of its customers were affected, each costing the corporation on average $125 per person to remedy the situation. On the government side, organizations are under the microscope of Congress for not taking adequate steps in protecting their customers' information. The list doesn't stop there though, organization such as the International Monetary Fund and defense contractors such as Lockheed Martin have also been recently exploited. It is no secret that the United States expects to receive millions of attacks every day, attempting to steal vital national security information and disrupt federal operations. Whenever data is sent electronically, it needs to be secured, which SE Enabled Technologies' software can do. These large organizations desperately need a viable solution in today's increasingly-digital world.

As the use of internet devices continues to grow past 80% of US citizens (Google), the frequency of attempted infiltration does as well. Enemies and allies alike recognize the vulnerability of the United States' cyber communications. With the United States' conventional military forces unmatched against almost every military on the planet, cyber communications is viewed as a large weakness. Soon, organizations and individuals will desire much better security solutions than are currently offered in order to combat and protect against the wave of attacks. SEET promises to deliver a security solution that is unmatched in the current marketplace. Utilizing Intel Labs' truly revolutionary Software Guard Extension technology, SE technologies will offer software solutions to provide an unmatched level of digital security for both individuals and large organizations.

Current competitive threats include existing endpoint security solutions, including established companies such as Symantec and AVG. However, these companies utilize software-based security solutions that have been proven to be vulnerable to sophisticated attacks. National security is an area that cannot afford any loss of data, so it requires a hardware-based solution.

Recommendations

There is the potential to exploit extremely lucrative opportunities utilizing our first-mover advantage in this emerging market segment. However, there is still significant work to be completed. The SE Enabled browser extension application is still in the early stages of development and numerous iterations will need to be completed before the software is fine-tuned. Therefore, we recommend continued research and development of existing and emerging technologies. We are currently negotiating with the Department of Veteran Affairs to conduct a $500,000 limited trial run of SE Enabled Technologies software as a proof of concept. If an agreement is

reached, it will mark a huge success that will give us the funds as well as the clout to commercialize SE Enabled software and to extend our services to other major organizations. To that end, much of our efforts will be directed towards reaching an agreement and accomplishing a proof of concept. We believe SE Enabled Technologies has tremendous opportunity to make an impact in the cyber security market. We remain confident that the coupling of Intel's SGX and SE Enabled Technologies software has the potential to transform cyber security on a global scale.

References

[1] United States. Cong. Senate Select Committee on Intelligence. Worldwide Threat Assessment of the US Intelligence Community: Statement for the Record, Senate Select Committee on Intelligence. By James R. Clapper. Cong. Rept. N.p.: n.p., 2013. Print.

[2] Hoekstra, Matthew, Et Al. "Using Innovative Instructions to Create Trustworthy Software Solutions." Intel.com. Intel Corporation, 2013. Web. 25 Feb. 2014.

[3] McKeen, Frank, Et Al. "Innovative Instructions and Software Model for Isolated Execution." Intel.com. Intel Corporation, 2013. Web. 25 Feb. 2014.

[4] Ibid.

[5] Hoekstra, Matthew, Et Al. "Using Innovative Instructions to Create Trustworthy Software Solutions." Intel.com. Intel Corporation, 2013. Web. 25 Feb. 2014.

[6] McKeen, Frank, Et Al. "Innovative Instructions and Software Model for Isolated Execution." Intel.com. Intel Corporation, 2013. Web. 25 Feb. 2014.

[7] MarketResearchMedia.com